(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : 2 689 662
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : 92 03941

(51) Int Cl⁵ : G 06 K 19/073

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 01.04.92.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 08.10.93 Bulletin 93/40.

(56) **Liste des documents cités dans le rapport de recherche** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *GEMPLUS CARD INTERNATIONAL Société Anonyme* — FR.

(72) **Inventeur(s)** : Foglino Jean-Jacques — *Cabinet Ballot-Schmit*, Imbert Patrick — *Cabinet Ballot-Schmit* et Kowalski Jacek — *Cabinet Ballot-Schmit.*

(73) **Titulaire(s)** :

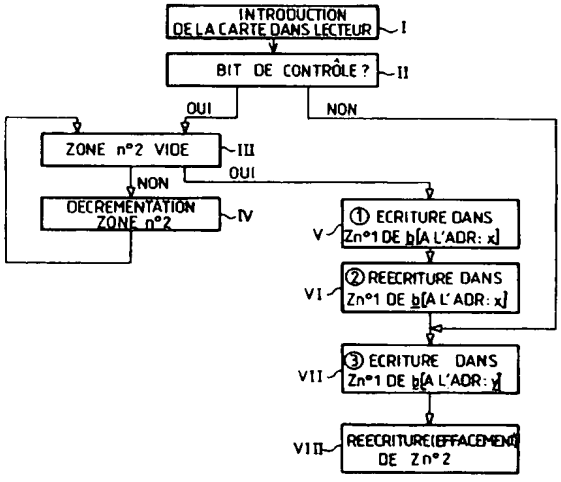
(74) **Mandataire** : Cabinet Ballot-Schmit.

(54) Procédé de protection d'une carte à puce contre la perte d'information.

(57) L'invention concerne un procédé de protection contre la perte d'information des cartes à puce du type cartes à comptage d'unités telles que les cartes téléphoniques ou les cartes de parcmètres en cas de mauvais fonctionnement du lecteur ou retrait intempestif de la carte.

Le procédé consiste à insérer dans la procédure de rechargement de la carte, l'écriture d'au moins un bit de contrôle pour témoigner de la réalisation effective du rechargement évitant ainsi qu'après l'écriture d'un bit de comptage et retrait intempestif de la carte, un rechargement ne soit perdu.

Application aux cartes à comptage d'unités.



FR 2 689 662 A1

1

PROCEDE DE PROTECTION D'UNE CARTE A PUCE CONTRE LA PERTE D'INFORMATION

La présente invention concerne un procédé de protection d'une carte à puce contre la perte d'information due notamment à un mauvais fonctionnement du lecteur ou à un retrait intempestif de la carte par l'utilisateur.

L'invention s'applique à des cartes à puce ayant une mémoire divisées en deux ou plusieurs zones de taille pouvant être différentes et dont l'écriture de l'une des zones est provoquée par une écriture dans l'autre zone.

On entend par écriture toute opération permettant d'une manière générale de modifier l'état d'un bit. Il s'agira donc soit d'une programmation, soit d'un effacement selon la technologie de la mémoire.

En pratique, dans une mémoire de ce type et telle que schématisée sur la figure 2, l'effacement d'une zone n° 2 est réalisé par la mise en oeuvre d'une séquence comportant les deux étapes suivantes :

1) - écriture d'un bit de comptage dans la zone n° 1,
2) - opération déclenchant l'effacement de la deuxième zone si l'écriture du bit de comptage a bien eu lieu.

En pratique cette opération consiste à réaliser une écriture du même bit au même emplacement dans cette même zone n°1.

C'est en effet, l'enchaînement de ces deux actions qui a pour effet l'effacement de la zone n° 2.

Dans de telles mémoires, la zone n° 1 permet d'effacer la zone n° 2, la zone n° 2 permet d'effacer la

zone n° 3 et ainsi de suite et cela grâce au mécanisme qui vient d'être décrit.

On rencontre ce type de fonctionnement par exemple dans les cartes de type cartes téléphoniques.

En effet, les cartes téléphoniques contiennent au moment de l'achat par l'utilisateur un nombre défini d'unités donnant droit pour cet utilisateur à des communications téléphoniques dont le nombre dépend du système de tarifications.

Or ces unités sont chargées dans une zone par exemple Z n°2 de la mémoire par l'écriture dans cette zone de n_2 bits. Au fur et à mesure des utilisations le nombre d'unité est décrémenté, les bits se trouvant dans un état binaire donné passent dans l'état complémentaire.

Lorsque la zone mémoire n° 2 chargée initialement est vide, l'enchaînement des opérations d'écriture sur la zone n° 1 décrites précédemment permet de recharger la zone n° 2 un nombre de fois égal au nombre de bits que l'on peut écrire dans la zone n° 1 dite zone de rechargement.

Le problème rencontré avec des mémoires dont le fonctionnement est de ce type est que si un mauvais fonctionnement du lecteur ou un retrait intempestif de la carte par l'utilisateur se produit avant la deuxième étape ou au cours de cette deuxième étape c'est à dire avant ou lors de la deuxième écriture du bit dans la zone n° 1 (zone de rechargement pour les cartes téléphoniques) alors le rechargement de la zone n°2 ne peut avoir lieu. La possibilité d'un rechargement est perdue pour l'utilisateur ce qui se traduit dans le cas de cartes téléphoniques par une perte du nombre d'unités téléphoniques correspondant à ce rechargement.

La présente invention a pour but de remédier à ce

problème.

La présente invention a pour objet un procédé de protection de carte à puce contre la perte d'information la carte comportant au moins deux zones de mémorisation, une première zone étant utilisée pour réécrire dans la deuxième zone lorsque le contenu de cette zone a été modifié par rapport à son contenu initial.

Selon le procédé une opération de réécriture de la deuxième zone à savoir, de la zone qui avait été chargée initialement, comporte les étapes suivantes :

1) écriture d'un bit de comptage dans la première zone, (zone qualifiée de rechargement),
2) effacement de la deuxième zone si l'écriture du bit de comptage a eu lieu,
3) écriture d'au moins un bit de contrôle, pour témoigner que l'étape 2) a bien eu lieu.

Le procédé consiste en outre, à chaque nouvelle introduction de la carte dans un lecteur à réaliser les étapes suivantes :

- vérification du (ou des) bit(s) de contrôle de l'étape 3) de la séquence précédente et selon son état, enchaînement des étapes qui n'ont pas été mises en oeuvre lors de cette séquence du fait d'un mauvais fonctionnement du lecteur ou d'un retrait intempestif de la carte de manière à réécrire dans cette deuxième zone son contenu initial.

Selon un autre aspect de l'invention l'écriture du (ou des) bit(s) de contrôle se fait dans la première zone c'est à dire dans la zone de rechargement de la deuxième zone.

Selon une première variante du procédé un seul bit de contrôle est écrit à chaque séquence et les adresses d'écriture du bit de comptage et du bit de contrôle se

succèdent, ces bits étant ainsi l'un à la suite de l'autre dans la zone de rechargement.

Selon une autre variante du procédé un seul bit de contrôle est écrit à chaque séquence et les adresses d'écriture du bit de comptage et du bit de contrôle sont dans des champs d'adressages disjoints dans cette zone de rechargement.

Selon une autre caractéristique de l'invention l'étape 2) consiste à réécrire le bit de comptage à la même adresse qu'à l'étape 1).

Selon une autre caractéristique de l'invention la vérification du bit de contrôle consiste à lire l'état de ce bit et en fonction de cet état de déclencher ou non une écriture de la deuxième zone.

Selon un autre aspect de l'invention, la carte à puce est une carte à comptage d'unités, la zone chargée initialement contient un ensemble de n_2 bits d'état identique correspondant à des unités d'utilisation, la zone permettant de réécrire la zone chargée initialement contentant un ensemble de n_1 bits. Le nombre de rechargements autorisés est égal à n1/2, les n1/2 autres bits étant des bits de contrôle.

Les caractéristiques et avantages de la présente invention apparaîtront mieux après la description qui suit, donnée à titre indicatif et nullement limitatif.

Cette description se réfère aux dessins annexés sur lesquels :

- la figure 1 est le schéma d'organisation d'une mémoire pour laquelle le procédé s'applique,
- la figure 2, représente un schéma du déroulement du procédé conforme à l'invention.

La figure 1 représente très schématiquement l'organisation d'une mémoire 1 d'une carte à puce 10. Le principe de son fonctionnement a été décrit

précédemment.

Le procédé conforme à l'invention s'applique à tout type de mémoire fonctionnant sur le principe déjà décrit, il s'applique notamment aux cartes à puce de type cartes à comptage d'unités telles que les cartes téléphoniques ou les cartes à parcmètre.

Selon l'invention la réécriture de la zone mémoire Z n° 2 (on peut parler également d'effacement ou de rechargement de la zone mémoire Z n° 2) est réalisée par l'enchaînement des opérations suivantes :

1) On écrit un bit $\underline{b}$ de comptage dans la zone Z n°1 de rechargement à une adresse x,
2) On réalise l'effacement de la zone Z n°2 si l'écriture du bit de comptage a bien eu lieu,
3) On écrit un bit $\underline{b}$ de contrôle dans la zone Z n° 1 de rechargement.
4) On vérifie à chaque nouvelle introduction de la carte l'état du bit de contrôle et en fonction de son état on recommence le procédé à partir de l'étape interrompue ou non commencée.

Tant que le procédé d'écriture n'a pas commencé, le bit de contrôle est correct. Dès que le bit de comptage a été écrit (étape 1), alors le bit de contrôle n'est plus conforme jusqu'à ce que l'étape 3) soit exécutée.

En pratique les opérations se déroulent de la façon suivante :

si le contenu initial de la zone Z n° 2 était de n_2 bits à l'état $\underline{b}$, ces bits sont passés à l'état $\overline{\underline{b}}$ au fur et à mesure des utilisations de la carte, l'opération de réécriture de cette zone (soit de l'effacement) permet de restaurer l'état initial et d'avoir n_2 bits à l'état b. Le nombre de réécriture de la zone est défini par le nombre de bits $n_1/2$ de la zone Zn°1.

- à chaque écriture d'un bit $\underline{b}$ à une adresse x dans

la zone Z n°1, on écrit selon un exemple particulier de réalisation également ce bit $\underline{b}$ dans cette zone Z n°1 à une autre adresse y, ce deuxième bit étant le bit de contrôle.

Lorsqu'un mauvais fonctionnement du lecteur, ou un arrachement intempestif se reproduisent entre l'étape 1 et l'étape 2 ou entre l'étape 2 et l'étape 3, le bit de contrôle ne peut être écrit. La relecture systématique de ce bit à chaque réutilisation de la carte permet de montrer qu'il n'y a pas concordance entre le bit de contrôle et le bit de comptage, l'état du bit de contrôle n'étant pas le même selon cet exemple.

En effet, l'état du bit de contrôle est $\overline{b}$, conformément au procédé on va alors modifier l'état de ce bit de manière à ce que l'écriture de ce bit de contrôle permette de réécrire les n2 bits de la zone Z n°2.

Selon un exemple de réalisation, l'étape 2) consiste à réaliser une deuxième écriture du bit de comptage par dessus celle qui a eu lieu à l'étape 1) à l'adresse x.

Après l'enchaînement des trois étapes, lorsqu'un nouvel enchaînement est déclenché par le lecteur de carte, bien entendu les adresses x et y sont incrémentées.

Les deux écritures du bit b à l'adresse x sont faites lors de l'enchaînement suivant, à une adresse qui est selon une variante du procédé l'adresse suivante x + 1.

Dans ce cas, le bit b de contrôle sera écrit dans un champ d'adresse disjoint du champ d'adresse dans lequel les deux écritures du bit b des étapes 1 et 2 se font.

Selon une autre variante du procédé, l'adresse

suivante est x + 2, le bit de contrôle étant écrit à l'adresse y = x + 1. Dans ce cas par conséquent le bit b et son bit de contrôle sont à des adresses successives.

Ce qui vient d'être décrit à propos des zones 1 et 2 peut être transposé aux zones 2 et 3 ...N - 1 et N.

Le déroulement du procédé conforme à l'invention a été représenté sur la figure 2 sous la forme de blocs fonctionnels I à VIII.

La présence du bit de contrôle (bloc II) se fait par comparaison de l'état de ce bit par rapport au bit b écrit à l'étape 1 ou 2 (blocs V ou VI) lors d'une introduction précédente de la carte.

Selon un autre aspect de l'invention, plusieurs bits de contrôle peuvent être écrit à l'étape 3) dans la zone de rechargement de la mémoire afin d'augmenter la sécurité du contrôle dans le cas de plusieurs retraits successifs de la carte.

Le procédé permet ainsi d'éviter toute perte d'information dans le cas de cartes du type à comptage d'unité telles que les cartes téléphoniques ou les cartes de parcmètre. Cette perte d'information se traduit par la perte d'une possibilité de recharger la carte comme cela se produit actuellement s'il y a un mauvais fonctionnement du lecteur ou un retrait intempestif de la carte.

REVENDICATIONS

1. Procédé de protection de carte à puce contre la perte d'information, la carte comportant au moins deux zones de mémorisation, une première zone étant utilisée pour déclencher une réécriture de la deuxième zone lorsque le contenu de cette zone a été modifié par rapport au contenu initial, caractérisé en ce qu'une opération de réécriture la deuxième zone comporte les étapes suivantes :

1) écriture d'un bit de comptage dans la première zone,

2) réécriture de la deuxième zone si l'écriture du bit du comptage a bien eu lieu,

3) écriture d'au moins un bit de contrôle pour témoigner que l'étape 2) a bien eu lieu, et caractérisé en ce qu'à chaque nouvelle introduction de la carte dans un lecteur, on réalise les étapes suivantes :

- vérification du (ou des) bit(s) de contrôle de l'étape 3) de la séquence précédente et selon son état, enchaînement des étapes qui n'ont pas été mises en oeuvre lors de cette séquence de manière à réécrire dans cette deuxième zone.

2. Procédé selon la revendication 1, caractérisé en ce que l'écriture du (ou des) bit(s) de contrôle se fait dans la première zone.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que l'étape 2) consiste à réécrire le bit de comptage à la même adresse qu'à l'étape 1).

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la

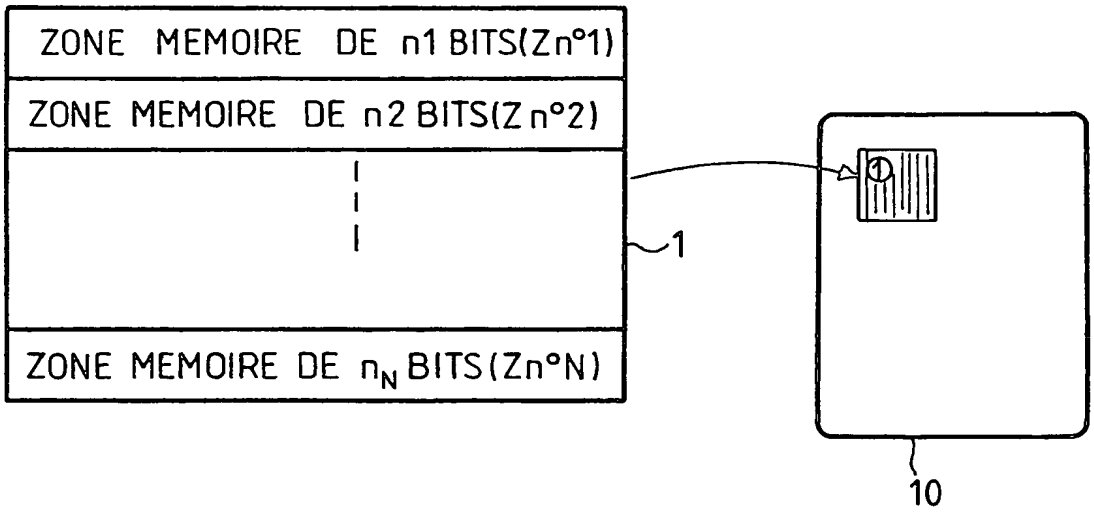
vérification du bit de contrôle consiste à lire l'état de ce bit et en fonction de cet état, de déclencher ou non une écriture de la deuxième zone

5. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'adresse d'écriture d'un bit lors des étapes 1, 2 et l'adresse d'écriture de ce bit lors de l'étape 3, se succèdent.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'adresse d'écriture d'un bit lors des étapes 1, 2 et l'adresse d'écriture de ce bit lors de l'étape 3, sont dans des champs disjoints.

7. Procédé de protection selon l'une quelconque des revendications précédentes dans lequel la carte est une carte à comptage d'unités, dans lequel la deuxième zone (Z n°2) est chargée initialement avec un ensemble de n_2 bits d'état identique correspondant à des unités ; dans lequel la première zone (Z n° 1) est chargée initialement avec un ensemble de n_1 bits de comptage d'état identique, caractérisé en ce que la réécriture de la deuxième zone permet de recharger cette zone et en ce que le nombre de rechargement de la carte par réécriture de cette zone est égal à la moitié de la taille de la première zone soit n1/2, l'autre moitié servant à écrire les bits de contrôle.

FIG_1



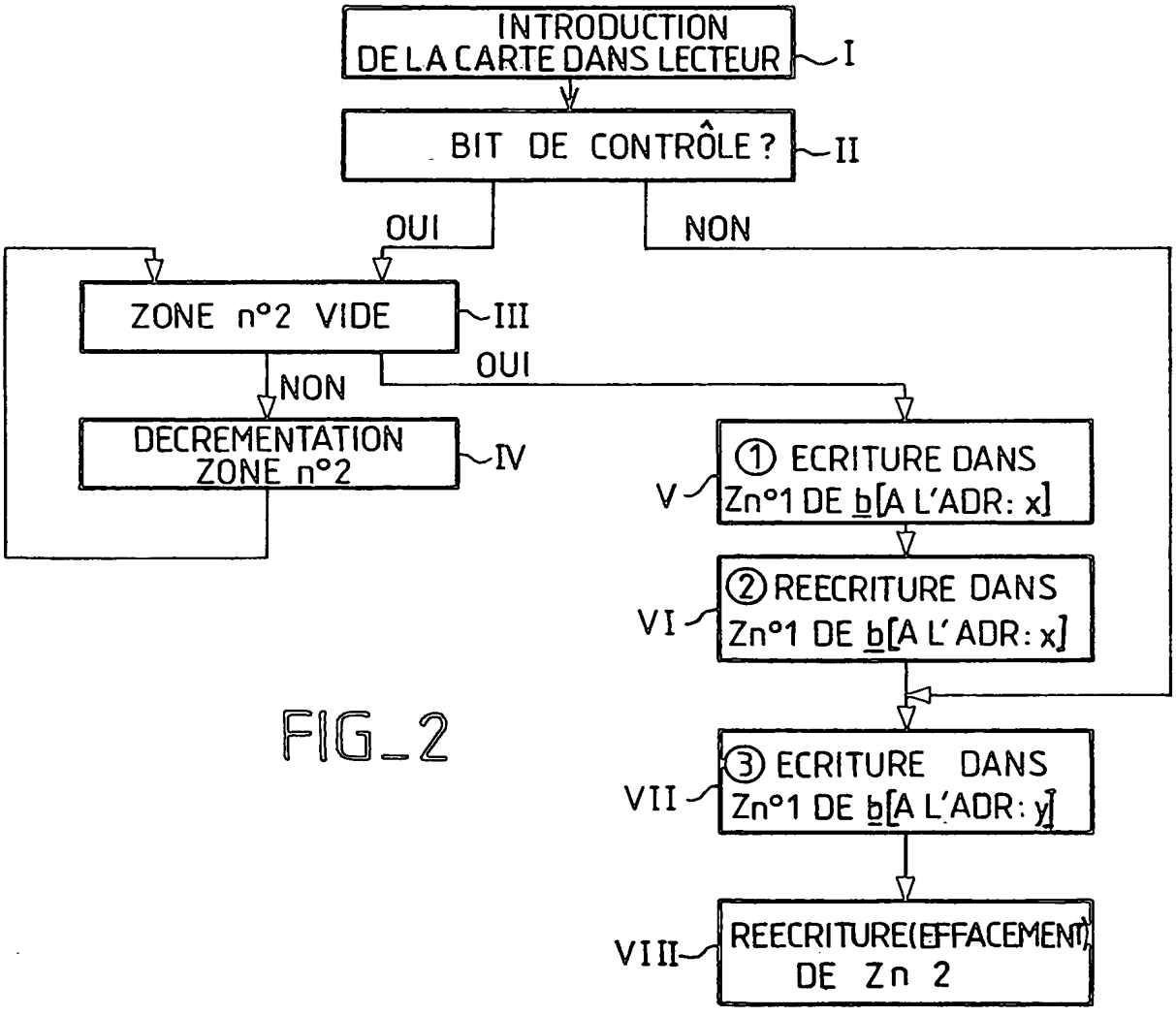


FIG_2

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2689662

N° d'enregistrement national

FR 9203941
FA 470907

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	DE-A-3 636 700 (KABUSHIKI KAISHA TOSHIBA) * résumé; figures 11A,B * ---	1
A	EP-A-0 227 532 (P. REMERY) * résumé; figure 4 * ---	1
A	WO-A-9 116 689 (N.V. NEDERLANDSCHE APPARATENFABRIEK) * résumé * -----	1

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G 06 K
G 07 F

Date d'achèvement de la recherche
24-11-1992

Examinateur
ZOPF K

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0413)